UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/077,365	02/15/2002	Gregory G. Rose	010027	3723

23696 7590 12/15/2006

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/077,365	ROSE ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29,44-48 and 55-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29,44-48 and 55-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 31, 2006 has been entered. Claims 1-29, 44-48, and 55-58 are pending. Claims 1 and 55 are amended by the applicant. Claim 30-43 and 49-54 has been cancelled by the applicant. At this time, claims 1-29, 44-48, and 55-58 are still rejected.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 55 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant recites "means for verifying the secure identifier, comprising:" in claim 55. It is not clear to the Examiner that whether the secure identifier or the means for verifying comprising the verifying steps of "mean for verifying that the public key ..... key identifier received; and means for verifying the time identifier .... Time tolerances." Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-2, 4-19, 44-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tello (US 6,463,537), and further in view of Hawkins et al (US 7,146,500).

a. *Referring to claim 1:*

i. Tello teaches:

(1) a processor **[i.e., referring to Figure 1, the major functional components of a typical motherboard comprises a CPU 101 (column 6, lines 22-23). Furthermore, the security engine 123 of this invention comprises a microprocessor with internal RAM (random access memory) and flash memory 125 and a scratch memory buffer 127 consisting of SRAM (Static Random Access Memory), a programming circuit 129 and independent battery backup circuit 131 (column 6, lines 40-45)]**;

(2) a clock coupled to the processor configurable to generate a time element **[i.e., the programming circuit 129 is logically connected to the security engine microprocessor 123, the security engine scratch memory 127, and the smart card reader 133 through the smart card interface 135. The smart card interface 135 is shown in Figure 2 and is comprised of PA0136, PB0138, PB1140, PB2142, PB3149 and Reset 150 lines which have pull down resistors on them, and Clock 152, Ground 154, and (Supply voltage) VCC 156 lines (column 6, lines 60-67 of Tello)]**;

(3) a memory element coupled to the processor configurable to store a private key and public key information **[i.e., also stored within the ROM are the same six encryption algorithms as are found in the flash memory of the security engine. The first is a public key based cryptographic algorithm that provides encryption and decryption for 48 and 64 bits of data (column 15, lines 5-10). The CK, which is stored in the internal memory of the smart card and the internal memory of the security engine, is used as an encryption key with an algorithm to encrypt or decrypt all communications after the first transfer of data between the security engine and the smart card (column 24, lines 31-35)]**;

(4) at least one actuator (e.g., a mechanism that puts something into automatic action, like battery backup circuit) coupled to the processor **[i.e., the battery backup circuit 131 connected to the microprocessor 125 allows the security engine 123 to always have automatic power on during interrupts such as during manual resets and power failures. This also ensures a secure and proper shut down procedure. This same battery also supplies the SRAM of the scratch memory 127. The scratch memory 127 is connected to the security engine microprocessor 125 through two lines. These two lines control the flow of data and address. The amount of data flow can easily be increased through the addition of more SRAM. A power on/power off circuit is connected to the microprocessor and the computer power supply. This allows the security engine to automatically power on during the start up of the computer or after an interrupt (column 6, lines 46-59)]**;

(5) a signature generator **(column 2, lines 55-59 of Tello)** coupled to the processor operable to generate a digital signature, the digital signature being a function of the private key and the time element; and an emitter (e.g., having a capability to send) coupled to the signature generator operable to emit the secure identifier, the secure identifier comprising the digital signature, time element, and public key information **[i.e., a `personalized` computer with a unique encrypted digital signature which will not boot up or recognize any data storage or communication peripheral devices without a matching `personalized` smart card containing a complementary encrypted digital signature (see abstract). The flash memory of the security engine's microprocessor contains six encryption algorithms. One algorithm is used for the generation of the hash number from the personalized information entered by the holder of a smart card during the initial security set up. This hash number is used in the identification and authentication of the user of this invention (column 7, lines 63-67 through column 8, lines 1-2). Upon power up or interrupt of the computer, the modified BIOS takes control and allows the security engine microprocessor to look for, and if present, read from a smart card in the smart card reader which is logically**

connected to the security engine microprocessor. If the smart card and the computer have not been previously `personalized` a security setup procedure is initiated and a unique hash number (digital signature) placed in the smart card during the initial set up of the security system and a complementary hash number similarly assigned to the security engine memory (column 5, lines 15-25). The level of access allowed is determined by the presence or absence of encrypted keys in the memory of the security engine which are required before any device driver can load and initialize and recognize its respective peripheral communication or data storage device. This enable and disable capability is achieved through the placement of enable/disable circuits between the peripheral device connector and its respective Bus. If the proper smart card is not present in the card reader, no device drivers will be loaded and the computer will not be operable (column 5, lines 35-44). Also stored within the ROM are the same six encryption algorithms as are found in the flash memory of the security engine. The first is a public key based cryptographic algorithm that provides encryption and decryption for 48 and 64 bits of data. This, and the same encryption algorithm stored in the security engine ensures that the initial data flowing between the smart card reader and the security engine microprocessor during the synchronization of communications is secure if intercepted (column 15, lines 6-13). In addition, Tello's invention also allows a `personalized` computer system that contains this invention to identify and authenticate another `personalized` computer connected to it in a network. In order to authenticate the identity of a second computer the first computer sends an identification request through application software which operates under the current operating system. This identification request is encrypted by a public key algorithm then forwarded through the network connection to the second computer (column 38, lines 21-29)].

ii. Although Tello teaches a clock in Figure 2 and a timer (column 7, line 61) and digital signature associates with the private key, Tello is silent

on the capability of showing digital signature being the function of the time element. Whereas, Hawkins teaches:

(1) Figure 2 of Hawkins shows the initial operation of the present system. Record 6 is sent from a remote location to the repository 5. Record 6 is receipted within repository 5 by prepending receipt 7 to the beginning of record 6 and appending receipt 8 to the end of record 6. In an exemplary embodiment, receipt 7 is the repository's digital signature of the combination of both record 6 and some identifying information. Receipt 8 includes the identifying information and a message digest of the combination of both record 6 and the identifying information. Identifying information can include a time-stamp and the originator of the record. All information that has been encrypted, including actual digital signatures in Figures 2 4, is shown in double-framed format **(column 6, lines 64-67 through column 7, lines 1-10 of Hawkins).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) combine the teaching of Hawkins into Tello's system to provide a method for revising authoritative electronic records that is secure, verifiable, and includes clear identification of involved parties **(column 6, lines 13-16 of Hawkins).**

iv. The ordinary skilled person would have been motivated to:

(1) combine the teaching of Hawkins into Tello's system to protect these systems and the data stored within them from unauthorized access and theft **(column 1, lines 26-27 of Tello).**

b. *Referring to claims 2:*

i. Tello teaches:

(1) a random number generator coupled to the processor to encrypt the digital signature **[i.e., upon start up of the computer system, an authentication procedure is executed by the microcircuit board in which identifies and authenticates the user through the verification of a smart card involving the**

comparison of encrypted keys created by the random number generator (column 2, lines 55-59)].

c. *Referring to claim 4:*

i. Tello teaches:

(1) further comprising an input element coupled to the processor, the input element capable of receiving a personal identification number (PIN) **[i.e., referring to Figure 1, keyboard, 117 and/or smart card reader, 133 are input elements].**

d. *Referring to claim 5:*

i. This claim has limitations that are similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

e. *Referring to claim 6:*

i. Tello teaches:

(1) further comprising a display coupled to the processor, the display capable of displaying key identifiers **[i.e., if a smart card is not present in the smart card reader a request to the user to insert a smart card is given via a display command sent to the BIOS 509 (column 25, lines 32-34). In addition, another command is sent to the BIOS to display the user identification set up screen 527. This screen displays a unique serial number assigned each security motherboard during its manufacture and allows the user to input personal information to be used to `personalize` each computer and smart card 529 (column 25, lines 62-67)].**

f. *Referring to claims 7-8:*

i. Tello teaches:

(1) wherein the secure identifier emitted is emitted as an audio tone or as an optical signal **[i.e., the three main methods by which a user's claimed identity is verified are through the use of: 1.) something the individual knows such as a password or PIN (Personal Identification Number); 2.) something the individual possesses, such as a token--a magnetic stripe card or smart card**

for example; and/or 3.) something unique to the individual, such as a biometric characteristic--retina pattern or fingerprint for example (column 2, lines 1-8)].

g. *Referring to claims 9-10:*

i. Tello teaches:

(1) wherein the actuator is a push-button switch or a voice activated switch **[i.e., three different lengths of communication are supported between the security engine microprocessor and the smart card reader. They are 1 byte, 6 bytes and 8 bytes. This allows the invention to be compatible with several different types of smart cards and to also support other identification and authentication devices such as button memory and biometric readers (column 16, lines 10-16)].**

h. *Referring to claims 11-13, 40-42:*

i. Tello teaches:

(1) wherein the public key information is a public key identifier; wherein the pubic key identifier is derived from the public key information; wherein the public key information is the public key **[i.e., this identification request is encrypted by a public key algorithm then forwarded through the network connection to the second computer. This request contains a request for selected identification data parameters which can be compared with the same parameters stored in a database of the requesting computer system. These parameters can include special identification codes that are stored in the Application area of the smart card. Upon receiving this request, the identification request is stored in the scratch memory buffer of the security engine and decrypted using the same public key algorithm as in the first computer. (column 38, lines 27-37)].**

i. *Referring to claims 14, 43:*

i. Tello teaches:

(1) wherein the digital signature is encrypted using a personal identification number (PIN) **[i.e., if the smart card and the computer have not been previously `personalized` a security setup procedure is initiated and a unique hash number (digital signature) placed in the smart card during the initial**

set up of the security system and a complementary hash number similarly assigned to the security engine memory. The hash number calculations are based on a set of personal information provided by the holder of a particular smart card and thus each computer and smart card is uniquely `personalized` for that user (column 5, lines 20-28)].

j. *Referring to claims 15 and 44:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

k. *Referring to claims 16, 45:*

i. Tello teaches:

(1) further comprising identifying a PIN, and wherein generating a digital signature is further a function of the PIN **[i.e., the three main methods by which a user's claimed identity is verified are through the use of: 1.) something the individual knows such as a password or PIN (Personal Identification Number); 2.) something the individual possesses, such as a token--a magnetic stripe card or smart card for example; and/or 3.) something unique to the individual, such as a biometric characteristic--retina pattern or fingerprint for example (column 2, lines 1-8)].**

l. *Referring to claims 17-18, 46-47:*

i. These claims have limitations that are similar to those of claims 7-8, thus they are rejected with the same rationale applied against claims 7-8 above.

m. *Referring to claims 19, 48:*

i. Tello teaches:

(1) wherein the digital signature is derived from a private key **[i.e., the security system involves the digital signing of adapter cards and ROM extensions for peripheral devices with the peripheral vendor's private key. During the ROM scan phase of the start up procedure of a computer, the BIOS compares a list of authorized public keys against the digital signatures of peripheral devices encountered during ROM scan. This requires that all**

approved peripheral devices be digitally signed with the vendor's private encryption key beforehand (column 4, lines 18-26)].

6. Claims 3 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tello (US 6,463,537), in view of Hawkins et al (US 7,146,500), and further in view of Akiyama et al (US 5,784,464).

a. *Referring to claims 3, 23:*

i. Although the combination of teaching between Tello and Hawkins teaches the claimed subject matter, they are silent on the capability of:

(1) wherein the time element comprises a predetermined number of least significant bits of the time.

ii. Whereas, Akiyama teaches:

(1) The key update timer 17 is a timer for regulating a timing of processing in the key update processing unit 16, as shown in Figure 3.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) combine the teaching of Akiyama into Tello's modified system to provide a client authenticating system for making the identification data impossible to be used by a third party by dynamically creating identification data used for the authentication between the user (client) and the service provider both in a client system and in a service provider system **(column 2, lines 11-16 of Akiyama).**

iv. The ordinary skilled person would have been motivated to:

(1) combine the teaching of Akiyama into Tello's modified system to protect these systems and the data stored within them from unauthorized access and theft **(column 1, lines 26-27 of Tello).**

7. Claims 20-29, 55-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tello (US 6,463,537), in view of Rabin et al (US 6,889,209 B1).

a. *Referring to claims 20, 26, 55:*

i. Tello teaches:

(1) a receiver configurable to receive a secure identifier **[i.e., the smart card interface circuit provides lines PA0, PB0, PB1, PB2, PB3,**

Clock, VCC, Ground and Reset which receive signals from an attached smart card reader 133. With communication lengths of 4, 6, and 8 bits available, the interface for different types of smart cards and other authentication and identification devices is provided (column 7, lines 45-52)], the secure identifier comprising:

(2) a digital signature, the digital signature comprising information derived from a private key, a public key identifier; and a time identifier **[i.e., if the smart card and the computer have not been previously `personalized` a security setup procedure is initiated and a unique hash number (digital signature) placed in the smart card during the initial set up of the security system and a complementary hash number similarly assigned to the security engine memory (column 5, lines 19-25). The level of access allowed is determined by the presence or absence of encrypted keys in the memory of the security engine which are required before any device driver can load and initialize and recognize its respective peripheral communication or data storage device. This enable and disable capability is achieved through the placement of enable/disable circuits between the peripheral device connector and its respective Bus. If the proper smart card is not present in the card reader, no device drivers will be loaded and the computer will not be operable (column 5, lines 35-44). Also stored within the ROM are the same six encryption algorithms as are found in the flash memory of the security engine. The first is a public key based cryptographic algorithm that provides encryption and decryption for 48 and 64 bits of data. This, and the same encryption algorithm stored in the security engine ensures that the initial data flowing between the smart card reader and the security engine microprocessor during the synchronization of communications is secure if intercepted (column 15, lines 6-13). In addition, Tello's invention also allows a `personalized` computer system that contains this invention to identify and authenticate another `personalized` computer connected to it in a network. In order to authenticate the identity of a second computer the first computer sends an identification request through application software which operates under the current operating system. This identification request is encrypted by a public key algorithm then forwarded**

through the network connection to the second computer (column 38, lines 21-29)]; and

(3) a verifier configurable to verify the secure identifier **[i.e., Tello's invention also allows a `personalized` computer system that contains this invention to identify and authenticate another `personalized` computer connected to it in a network. In order to authenticate the identity of a second computer the first computer sends an identification request through application software which operates under the current operating system. This identification request is encrypted by a public key algorithm then forwarded through the network connection to the second computer (column 38, lines 21-29)]**, the verifier comprising:

(4) memory comprising information corresponding to the public key information received and time tolerance information **[i.e., also stored within the ROM are the same six encryption algorithms as are found in the flash memory of the security engine. The first is a public key based cryptographic algorithm that provides encryption and decryption for 48 and 64 bits of data (column 15, lines 5-10). The CK, which is stored in the internal memory of the smart card and the internal memory of the security engine, is used as an encryption key with an algorithm to encrypt or decrypt all communications after the first transfer of data between the security engine and the smart card (column 24, lines 31-35)];**

(5) a key retriever coupled to the memory and configurable to retrieve a public key corresponding to the public key identifier **[i.e., writing the retrieved identification data to the internal memory of the security engine microprocessor (column 46, lines 24-25)];** and

(6) a time verifier (e.g., timer for verifying time) coupled to the memory and configurable to verify that the received time identifier falls within acceptable time tolerances **[i.e., an interrupt line leads from the security engine microprocessor to various circuits which control the interrupt for the computer CPU, reset, on-off, detecting the presence of a smart card in the reader, and timer (column 7, lines 58-61)].**

ii. Although Tello teaches a clock in Figure 2 and a timer (column 7, line 61) and number of data bits in cryptographic algorithm, Tello is silent on the capability of showing:

(1) time tolerance information.

iii. Whereas, Rabin teaches:

(1) The guardian center may also verify that the received time is within a specified tolerance of the clock time on the guardian center **(column 7, lines 7-9 of Rabin).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) combine the teaching of Rabin into Tello's system since the time is stored in the continuation message and the time is verified to be earlier than by less than a specified value from the user device time upon receiving the continuation message **(column 9, lines 18-21 of Rabin).**

v. The ordinary skilled person would have been motivated to:

(1) combine the teaching of Rabin into Tello's system to protect these systems and the data stored within them from unauthorized access and theft **(column 1, lines 26-27 of Tello).**

b. *Referring to claims 21, 27, 56:*

i. Tello teaches:

(1) the secure identifier further comprises a PIN **[i.e., the three main methods by which a user's claimed identity is verified are through the use of: 1.) something the individual knows such as a password or PIN (Personal Identification Number); 2.) something the individual possesses, such as a token--a magnetic stripe card or smart card for example; and/or 3.) something unique to the individual, such as a biometric characteristic--retina pattern or fingerprint for example (column 2, lines 1-8)]**, and wherein the receiver is configurable to decrypt the digital signature using the PIN **[i.e., all tasks involving a peripheral device pass through this address space and it is here that all encryption and decryption operations take place controlled by the security engine (column 9, lines 5-8)].**

c. *Referring to claim 22:*

i. Tello teaches:

(1) wherein the key retriever compares the public key identifier received to public key information stored in memory [i.e., when the registers are read from the smart card to determine the type of card is inserted, an encrypted code number is read from the register of the inserted smart card and decrypted by the security engine microprocessor using the public encryption key 475. This code is then compared to a table of smart card code numbers that are stored in flash memory in the security engine 477. From this comparison, the type of smart card can be ascertained. By default, all smart cards, with the exception of vendor smart cards, have the code for a `new` card in the appropriate register location until changed through the set up procedure (column 24, lines 46-56)].

d. *Referring to claims 24-25, 28-29, 57-58:*

i. These claims have limitations that are similar to those of claims 7-8, thus they are rejected with the same rationale applied against claims 7-8 above.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Novicov et al (US 6,275,934 B1) discloses authentication for information exchange over a communication network (see title).

b. Kobayashi (US 7,093,131 B1) discloses information authenticating apparatus and authenticating station (see tittle).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
December 11, 2006

Thanhnga B. Do
AU2135